POLICY TITLE: Acceptable Use of Information and Communication Technology Resources

DATE DRAFTED: 11th December 2009

DATE APPROVED:

DATE REVISED:

PURPOSE

Makerere University has over time invested in Information and Communication Technology infrastructure in an effort to improve its administrative, teaching, learning and research functions. The University considers Information and Communications Technology (ICT) resources to be a valuable asset whose use must be managed to ensure their integrity, security and availability for lawful educational and administrative purposes.

While the university seeks to promote and facilitate the use of ICT resources, such use must be responsible and must respect the rights of other users. This document is provided to give guidelines to users of information technology resources, without compromising on the principles of academic freedom and free exchange of ideas.

SCOPE

This acceptable use policy applies to all users of the University's ICT resources. The resources referred to in this policy include but are not limited to:

- The Network and related network services

- University Computers and related peripherals

- Information systems including the Integrated Tertiary Education Information System and the Library Information system

- The University databases

- Learning management systems

- Any other system that may be installed to provide a service on the University network.

Users of ICT resources in this case are defined as any individual who uses or attempts to use the ICT resources described herein, and may include University students, members of staff and individuals who are not members of the University community but have been granted temporary use of the University resources. The

definition also covers any individual who connects, attempts to connect to or traverses the University network whether from within the University or from a remote location.

USER RESPONSIBILITIES

Makerere University ICT resources are provided primarily to facilitate a person's work as an employee or student or other role within the University. Use for other purposes, such personal or recreational use is a privilege, which can be withdrawn. In all cases, users are obliged to use resources responsibly to ensure their availability to other users.

Acceptable use of the University ICT resources

Acceptable use of the University ICT resources may include:

- Use for official University business;

- The use for academic and research work;

- Recreational use as long as it is in keeping with the framework defined in this policy, and such use does not interfere with one's duties, studies or the work of others

Unacceptable use of the University ICT RESOURCES

Unacceptable use of the university's ICT resources may include but are not limited to:

- Attempts to break into or damage computer systems within the network or in other connected networks;

- Attempts to access computers for which the individual is not authorized;

- Unauthorized access to another users files;

- Attempting to circumvent Network Access Control, including by-passing proxies and firewalls;

- Monitoring or interception of network traffic without permission;

- Probing for the security weaknesses of systems by methods such as port-scanning, password cracking, without permission

- Unauthorized extension or retransmission of network traffic including the installation of unauthorized wireless access points, routers or switches;

- Unauthorized reselling of network and Information Management systems services;

- Unauthorized modification of university's data

- Unauthorized download, installation or running of programs or utilities that may flood the network, causing denial of service to other users

- Sharing of network access credentials with third parties for purposes of defeating network authentication;

- Using the network to break into other networks

- Creation, retention, downloading or transmission of any offensive, obscene or indecent images or data, or any data capable of being resolved into obscene or indecent images or material;

- Creation, retention or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety;

- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;

- Sending electronic mail that purports to come from an individual other than the person actually sending the message using, for example, a forged address;

- Using the resources for unsolicited advertising or transmission of electronic mail with intent to defraud, often referred to as "spamming";

- Deliberate unauthorized access to networked resources, local or remote;

- Deliberate activities that may result to one of the following

  - Wasting of support staff time in support of systems

  - Corrupting or destroying other users data

  - Violating the privacy of other users

  - Denying services to other users

- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software;

- Download, installation and use of unlicensed software on the University network and computers